LA-UR 91 2403 CONF-910717--7

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--91-2403

DE91 016011

TITLE: A NETWORK SECURITY CASE STUDY: THE LOS ALAMOS NATIONAL LABORATORY INTEGRATED COMPUTER NETWORK

AUTHOR(S): J. S. Dreicer and L. Stoltz

SUBMITTED TO: 32nd Annual Meeting of the Institute of Nuclear Materials Management, New Orleans, Louisiana, July 28-31, 1991

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

A NETWORK SECURITY CASE STUDY: THE LOS ALAMOS NATIONAL LABORATORY INTEGRATED COMPUTER NETWORK*

Jared S. Dreicer and Laura Stoltz
Safeguards Systems Group
Los Alamos National Laboratory
Los Alamos, New Mexico 87545, USA

ABSTRACT

A study to validate the Graphical Network Representation (GRPHREP) model is being conducted on the Los Alamos National Laboratory Integrated Computer Network (ICN). The GRPHREP model is a software system application based on graph theory and object-oriented programming methodologies. It codifies the Department of Energy (DOE) Order 5637.1, which is concerned with classified computer security policy, restrictions, and requirements. The Los Alamos ICN is required to control access to and support large-scale scientific and administrative computing. Thus, we felt that this large, complex, and dynamic network would provide a good test for the graphical and functional capabilities of the model. Furthermore, the ICN is composed of multiple partitions that reflect the sensitivity and classification of the computation (data) and designate the required clearance level for the user. The determination of the sufficiency of these classification and clearance restrictions in conjunction with the ICN partitions supplied an excellent opportunity to exercise the implementation (codification) of Order 5637.1. During the study, we corrected the shortcomings of the model that were demonstrated; most were minor implementation issues. However, we discovered one major deficiency, the lack of specific network security servers; we incorporated this feature into the model.

I. INTRODUCTION

The Graphical Network Representation (GRPHREP) model is a computer-based tool that provides the capability to

*This work was supported by the US Department of Energy, Office of Safeguards and Security.

investigate and determine security concerns related to computer networks in particular and graph structures in general.[1] This tool can also be applied to problems other than security that are characteristic of graph structured problems, such as design, path routing, scheduling, network control, cycle generation, connectivity, resource contention, and traversability.[2] The analytical foundation of the GRPHREP model is based on graph theory; abstractly, networks, distributed systems, and parallel machines are specific graph theoretical problems. A graph $G = (V, E)$ is a structure that consists of a finite set of vertices V and a finite set of edges E (an edge is specified by an unordered pair of distinct vertices).[3-7] In the GRPHREP model, networks are fundamentally represented and characterized in terms of graph theory and graph structures. A network $N = (C, L)$ is a structure that consists of a finite set of components C and a finite set of links L (a link is specified by an ordered/unordered pair of distinct components). A similar transformation is possible for distributed systems, $D = (C, L)$, and parallel machines, $P = (C, L)$, where C and L are as previously defined. In GRPHREP, our definition of a computer network is very general. It is any collection of interconnected, autonomous computers or components of hardware (e.g., CPUs, memory, printers, disk storage components, or plotters). If two or more computers or components are able to exchange information, then they are interconnected. This definition of a computer network complements the definition of a graph structure.

The rapid emergence of large heterogeneous networks, distributed systems, and massively parallel machines has resulted in economies of scale, enhanced productivity, efficient communication, resource sharing, and increased reliability, which are computationally beneficial. However, networking presents technical challenges and problems with respect to maintaining and ensuring the security, design, compatibility, integrity, functionality, and management of these systems. Although the GRPHREP system was originally developed to address network security concerns, it has become obvious that GRPHREP could be used to assist in performance analysis, engineering design, and system management of networks. Additionally, the incorporation of network security servers has demonstrated the feasibility of including the representation of distributed systems and parallel machines in the model.

II. NETWORK SECURITY

Network security was initially addressed in the GRPHREP model by combining two distinct approaches. The first approach concentrated on network security in terms of the security of each stand-alone component. The second approach dealt with network security from a systems perspective. In this perspective a network is viewed as the combination of various sub-systems, in which each component and each link of a network are sub-systems that have specific requirements and risks associated with them. This systems perspective permits the security features of the heterogeneous sub-systems to be evaluated in terms of a homogeneous network. In general, the combination of these two approaches in the GRPHREP model is sufficient to determine the security of small and simple networks. However, for large and complex networks that include some sort of hierarchical security service, it is deficient. It became evident that some representational and functional capabilities had been omitted in determining network security in the GRPHREP model during the validation study of the Los Alamos National Laboratory Integrated Computer Network (ICN). This omission was due to the size, complexity, and requirements of the ICN and to the operational network security practices and methodologies used at the facility. The modification of the GRPHREP model to include the representational capabilities and functionality of network security servers reflects their use in the operational network security for the ICN. The implementation of network security service in the GRPHREP model expanded on the existing two approaches; the stand-alone and the systems perspective.

A. Stand-Alone Approach

The security risks for a stand-alone component are related to data integrity, data sensitivity, and computer access. The security determination for a stand-alone computer is a function of user clearance level, data classification level, the computer's evaluated product list (EPL) level, the operating mode of the computer, and a protection index. Users of a computer are assigned clearance levels and need-to-know permission that allows read/write access to data in the computer. The data stored and processed on a computer are assigned a classification level that reflects the importance of protecting their integrity, that is, preventing destruction, disclosure, or modification of the data. The EPL level of a computer indicates its ability to prevent an unauthorized user from accessing data and indicate the attempt. The operating mode of a computer is either dedicated, system high, compartmented, or multilevel. The protection index depends on the user clearance level and the data classification level relative to the EPL level of the computer on which the data are stored and processed. The protection index reflects the inherent vulnerability of the data to access on a particular computer. Using the protection index, it is possible to specify the minimum acceptable EPL level that is needed to keep the data from being vulnerable. Because the protection index is a function of the user's clearance and data classification levels, the security requirements for a stand-alone computer translate into the protection index indicating the required minimum EPL level that the computer must meet. Algorithms to determine the appropriate operating mode and EPL level for a stand-alone computer were codified in the GRPHREP model.

B. Systems Approach

A network is composed of individual subsystems (components) interconnected by links, hence each subsystem (component) in the network has stand-alone security risks (data integrity, data sensitivity, and computer access) in addition to network security risks, such as the propagation of local risk. The propagation of local risk is related to the possibility of a vulnerability on an individual computer propagating to one or more computers linked in the network. The propagation of local risk can cause a network vulnerability to appear as if it were a stand-alone machine vulnerability. The security determination from the systems perspective is a function of the link classification level and the user clearance levels, data classification levels, the machine's EPL levels, the operating modes, and the protection indices of the interconnected components. Algorithms to determine the interconnection security and compatibility between subsystems (components) and across links were codified in the GRPHREP model.

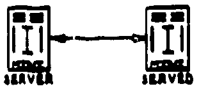
The stand-alone security approach ensures the compliance with policy concerning the use of various operating modes and the necessary hardware and software functions associated with particular EPL levels relative to data classification and user clearance levels. The security approach from the systems perspective ensures data transfer compatibility and security over a link, and the compatibility of the operating mode, data classification, and use: clearance between subsystems. The combination of these two approaches allows for the evaluation of security in a network by determining the requirements and restrictions for each subsystem and then assessing the effect of interconnectivity. This is accomplished in part by the existence or absence of the following features: authentication, access control, auditing, and internal labeling for each subsystem and the effect of a particular feature in terms of interconnectivity. During the ICN validation study, an important concern was not only the existence or absence of these features in subsystems but also the capability of subsystems to either inherit or transfer these features. In the ICN, certain distinct and dedicated subsystems provide (serve) the following security features: authentication, auditing, and assurance testing to other subsystems.

III. NETWORK SECURITY SERVICE

The network security service developed in the GRPHREP model is a reflection of the functionality manifested in the ICN. The network security service is not similar to the conventional client-server model under which print and file servers typically operate. The client-server model relies on the client to request services through an interface and for the server to provide services defined by the interface.[8-10] Instead, the network security service is more of a hybrid, that is, it is an integrated interconnected resource sharing service. Thus, network security service is not exactly like file servers and print servers in networks and distributed systems, but is similar in concept.

In GRPHREP, our characterization of a network security service is very general and simple. It builds on the existing definition of a network and does not cause any fundamental changes to the analytical basis of the model. A network is any collection of two or more interconnected subsystems (components). Interconnection indicates the ability to exchange information or, in this instance, services. Thus, network security service is the ability to provide security checking actions on served components with the computation executed on server components. This definition of a network security service conforms to the definition of a network in that it merely expands the capacity of components, *C*. The server can only check the security features that are resident on it and those served to it by any other server. Similarly, the checking capability of the served component is limited to the security features resident on it and the features served to it by any server. Service is really a formalism for the computational operation of controlling and exchanging predetermined, situation-specific information. An example will clarify this abstraction.

For example in Fig. 1, machine SERVER is interconnected with machine SERVED. Machine SERVER has user identification and authentication controls (class C1) and machine SERVED does not (class D). However, it is desirable to check the user identification and authentication on SERVED. Because SERVER and SERVED are interconnected, this is accomplished by making SERVER a network security server, effectively passing the user identification and authentication feature to SERVED. In reality, SERVER conducts the computational operation of user identification and authentication for SERVED. Furthermore, to preserve space-time requirements, SERVER requires that the user's actual login password (authentication) be given after the user name has been entered (identification).



Security Server	yes	no
ID-Authentication	yes	yes - served from SERVER
Audit Trail	no	no
Access Controls	no	no
Internal Labels	no	no
Assurance Testing	no	no

Fig. 1. Server–served relationship

The GRPHREP model has been modified and enhanced to accommodate the inclusion of network security services. Abstractly, a network security service subsystem can be thought of as providing hierarchical security protection to subordinate subsystems in addition to their existing protections.

IV. VALIDATION STUDY

The validation study for the GRPHREP model consisted of modeling the Los Alamos National Laboratory ICN, which controls access to and supports large-scale scientific and administrative computing. The ICN is composed of four partitions that reflect the sensitivity and classification of the computation (data) and designate the required clearance level for the user. The designations for the four partitions are secure, national security, administrative, and open. The following is a general description of the partitions: secure partition is for classified and unclassified computing by Q-cleared users; national security partition is for classified and unclassified computing by DOD secret-cleared (or equivalent) users; administrative partition is for unclassified and confidential (personnel records) computing by Q-cleared users; and the open partition is for unclassified computing by any authorized user.

The ICN interconnects a diverse array of state-of-the-art and sophisticated computing resources (subsystems), as shown in Fig. 2. The hardware includes a large number of worker machines, including Cray, CDC Cyber, Thinking Machine (parallel machine), and VAX computers; specialized communications networks; data storage facilities; and hardcopy facilities. These user facilities are supported by specialized computers for security, file switching, and port selection. The worker computers are connected through the File Transport (FT) Servers to the Common File System (CFS), the Print and Graphics Express Station (PAGES), and the Facility for Operations Control and Utilization Statistics (FOCUS). The ICN has the capability to communicate with other facilities using the eXtended NETwork (XNET).[11] Additionally, various operating systems are employed on the worker machines including CTSS (Cray's), NOS (CDC Cyber's), UNIX, and VMS. This network is composed of a very large number of heterogeneous subsystems all operating (usually) in a homogeneous manner.

The determination of the sufficiency of the various classification and clearance restrictions in conjunction with the ICN partitions and the high degree of interconnectivity supplied an excellent opportunity to exercise the GRPHREP model. The high degree of interconnectivity in the ICN

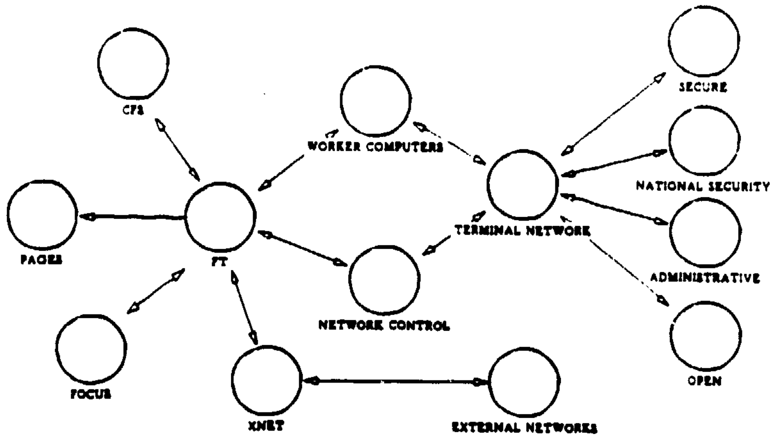


Fig. 2. Los Alamos National Laboratory ICN

necessitates the control of information flow, which is restricted to flow from a lower partition to higher partition. Resourcє protection is also strictly concerned with usєr validation, with respect to user identification and authorization in combination with partition access. Each subsystem has security features resident and active on that subsystem, in addition to being served various security features by other dedicated subsystems. As seen in Fig. 3, the network security controller conducts a variety of functions including user identification and authorization and access control.[12]

V. CONCLUSIONS

Now that the GRPHREP model includes representational and functional capabilities for network security service, it is complete in terms of a network security model. These capabilities have enhanced and strengthened the utility of the model with respect to conducting security studies and analyzing existing and proposed networks. In GRPHREP our characterization of a network security service is general and simple. It builds on the existing definition of a network and does not fundamentally change the analytical basis of the model. The ICN validation study has proven the value and demonstrated the power and applicability of the GRPHREP model for security studies. Because the ICN is a large, multilevel, complex, and dynamic network with explicit security requirements (due to the national security nature of the information processed at Los Alamos), it is proving to be an extremely demanding test

Security Server	yes
ID-Authentication	yes
Audit Trail	yes
Access Controls	yes
Internal Labels	yes
Assurance Testing	yes

Fig. 3. ICN Network Security Service

case. Furthermore, the methodologies and techniques employed to incorporate the network security service representation provide insight into the difficulties that will be encountered and the initial steps required to develop a complete model of distributed or parallel systems. The implementation of network security service can be viewed as a first step in attempting to develop a model of distributed system functionality. The network security service is an integrated, interconnected, resource-sharing, hybrid service.

In the future, complete representational and functional capabilities for distributed or parallel systems should be implemented for the GRPHREP model. The logical and prudent choice is to first implement a complete representation of distributed systems. Once this has been accomplished, it would be possible to use those representational capabilities to model massively parallel systems. This work should be implemented on the original GRPHREP model system resident on a Texas Instrument Explorer. Once the proof-of-concept for these principles has been demonstrated, modification could be initiated on the Graphical Network Security System (GNETS).[13]

The GNETS system is a PC delivery system. The software is coded in Zortech C++ and has been designed to execute on a PC 286 or clone PC compatible. The GNETS system closely replicates the functionality and capability of the GRPHRREP system.

REFERENCES

1. J. S. Dreicer, W. Smith, and L. Stoltz, "Network Security and the Graphical Network Representation Model," in *Proceedi ıgs of the 13th National Computer Security Conference* (National Computer Security Center, Ft. George G. Meade, Maryland, 1990), Vol. I, pp. 243-252.

2. J. S. Dreicer, "Graph Structure Model," *Nucl. Mater. Manage.* **XIX**, 43-46 (1990).

3. M. F. Capobianco, M. Guan, D. F. Hsu, and F. Tien, Eds., "Graph Theory and Its Applications: East and West," *Proceedings of the First China—USA International Graph Theory Conference* (New York Academy of Sciences, New York, 1989).

4. M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, San Francisco, 1979).

5. E. L. Lawler, J. K. Lenstra, A. H. G. Rinnooy Kan, and D. B. Shmoys, *The Traveling Salesman Problem—A Guided Tour of Combinatorial Optimization* (Wiley, Great Britain, 1985).

6. T. Nishizeki and N. Chiba, *Planar Graphs: Theory and Algorithms* (North-Holland, Amsterdam, 1988).

7. R. J. Wilson and L. W. Beineke, *Applications of Graph Theory* (Academic Press, London, 1979).

8. S. Krakowiak, *Principles of Operating Systems* (MIT Press, Cambridge, Massachusetts, 1988).

9. L. Bic and A. Shaw, *The Logical Design of Operating Systems* (Prentice Hall, New Jersey, 1988.

10. J. Peterson and A. Silberschatz, *Operating System Concepts* (Addison-Wesley, Massachusetts, 1983).

11. T. Spitzmiller, "Catalog of ICN Resources," Los Alamos National Laboratory document CIC #212 (November 1987).

12. K. Jackson and D. Merrigan, "Network Security Controller Upgrade Requirements Document," Los Alamos National Laboratory, Computer Network Engineering Group internal document (December 1989).

13. L. Stoltz, "GNETS: Graphical Network Security System—User Guide," Los Alamos National Laboratory, Safeguards Systems Group report (1991).